REMARKS

Claims 1-6 and 8-21 are pending in this application. By this Amendment, claims 1, 9-13, 17 and 20 are amended, and claims 7 and 22 are canceled without prejudice or disclaimer to the subject matter set forth therein.

No new matter is presented by this Amendment. Support for the amendments may be found, for example, in the Abstract and in paragraphs 0009, 0012, 0021, 0039-0052, 0069-00076 and 0094 of the published patent application US 2003/0105981 and in the drawings, for example.

Applicant respectfully requests reconsideration of the application.

A. The 35 U.S.C. §112, first paragraph, Rejection

In the Office Action, claims 1-22 are rejected under 35 U.S.C. 112. first paragraph. as failing to comply with the written description requirement. The Office Action asserts that the claims contain subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Applicant has amended the claims in response to the Examiner's comments and suggestions. It is respectfully submitted that in view of the amendments, the rejection under 35 U.S.C. §112, first paragraph, is obviated. Applicant submits the claims satisfy all requirements of 35 U.S.C. §112. Withdrawal of the 35 U.S.C. §112 rejection is respectfully requested.

B. The 35 U.S.C. §112, second paragraph, Rejection

In the Office Action, claim 1 is rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential elements, such omission amounting to a gap between the

elements. The Office Action asserts the claim recites the step of "the first system presenting at least some of the information from the session token to the second system" followed by "the first system determining whether the client has a valid session credential granted by the second system". The Office Action sets out that there appears to be a missing step, because it is unclear how or what is communicated from the second system to the first system that would enable the first system to determine whether the client has a valid session credential.

Applicant has amended the claims in response to the Examiner's comments and suggestions. It is respectfully submitted that in view of the amendments, the rejection under 35 U.S.C. §112, second paragraph, is obviated. Applicant submits the claims satisfy all requirements of 35 U.S.C. §112. Withdrawal of the 35 U.S.C. §112 rejection is respectfully requested.

C. The 35 U.S.C. §103 Rejection

In the Office Action, claims 1-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Howard et al. (hereinafter Howard) U.S. Patent 6,584,505 in view of Wood et al. (hereinafter Wood) United States Patent Number 6,668,322. This rejection is respectfully traversed.

With reference to claim 1, the Office Action asserts that Howard teaches a method for validating credentials comprising determining, at a first system that grants session credential based on successful authentication at the first system or successful authentication at a second system, that a client does not have a valid session credential by the first system; (col. 6, lines 46-50; col. 8, lines 41-43); retrieving, at the first system, information from a session token held

by the client, the information corresponding to a possible session credential for the second system that grants session credentials based on successful authentication at the second system; (col. 6, lines 51-52); the first system presenting at least some of the information from the session token to the second system; (col. 6, lines 51-52; col. 8, lines 54-57) and the first system determining whether the client has a valid session credential with the second system; and (col. 8, lines 2-7; col. 8, lines 41-43; col. 8, line 66 - col. 9, line 6) determining at the second system whether the client has a valid session credential granted by the first system, so as to authenticate at the second system. (col. 9, lines 16-23)

The Office Action notes that Howard does not explicitly disclose a session token, but that Wood in analogous art, however, discloses a session token. (col. 3. lines 2-12). The Office Action concludes that it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Howard with Wood in order to provide a system that allows inspection of credentials by a wide variety of entities or application to an authenticated trust level while preventing alteration except by a trusted authentication service.

Claim 1 is amended to further clarify the claimed invention. As recited and shown above, claim 1 is directed to a method for validating credentials. In particular, claim 1 recites retrieving, at the first system, information from a session token held by the client, the information being retrieved from the client, the information corresponding to a session credential for the second system, the second system (1) grants session credentials based on successful authentication at the second system, and (2) includes a protected resource on the second system that is accessible by the client.

Howard fails to teach or suggest the claimed invention. As discussed in the Abstract, Howard describes that the system determines whether to grant access to a network server by a user. Howard describes that initially, a user attempts to gain access to a network server, such as a web server. Prior to granting access to the network server, the network server authenticates the user by sending an authentication request to an authentication server. The authentication server determines whether the user was already authenticated by the authentication server. If the user was already authenticated by the authentication server, then the network server is notified that the user is authenticated. The network server then grants the user access to the network server. If the user was not already authenticated by the authentication server, then login information is retrieved from the user and compared to authentication information maintained by the authentication server. If the retrieved login information matches the authentication information, then the network server is notified that the user is authenticated.

Accordingly, such teaching of Howard relies on interaction with an "authentication server". Such is in contrast to the claimed invention. Specifically, claim 1 recites that the second system includes a protected resource on the second system that is accessible by the client. Such distinguishes claim 1 from Howard, i.e., the authentication server of Howard has no protected resource that the client may access, as is claimed. Such language of claim 1 further reflects the architecture of the invention that the fist system is essentially impersonating the client in the interaction of the first system with the second system. Such architecture is in sharp contrast to the arrangement of Howard utilizing a central authentication server.

In column 6, lines 38-52, Howard teaches that Fig. 4 of Howard is a flow diagram illustrating the authentication process when a user of the client computer system 100 seeks

access to the affiliate server 104. Howard describes the process begins when the user of the client computer system accesses a web page on the affiliate server (step 200). The client computer system includes a web browser for accessing various web sites. The affiliate server determines whether the user seeking access to the server is already logged into the affiliate server (e.g., authenticated) at step 202. In this example, the user is not logged into the affiliate server, so the user must be authenticated before the affiliate server will allow access. To authenticate the user, the affiliate server *redirects* the user's browser to the authentication server. Thus, this manipulation of the user is different than the claimed invention, i.e., in the claimed invention the first system presents information (from the client) to the second system.

Yet further aspects of Howard are described in column 8, lines 38-67. In this example of Howard, the user of the client computer system 100 accesses a web page on the affiliate server 104 (step 230). The affiliate server determines that the user is not authenticated (with respect to the affiliate server) and redirects the user's browser to the authentication server (step 232). Next, the authentication server retrieves the affiliate information entered during registration of the affiliate to determine whether the most recent authentication of the user is within the affiliate's timeout period (step 234). If the most recent authentication is not within the timeout period (i.e., not acceptable), then the authentication server retrieves and authenticates the user's login ID and password (step 238) using, for example, the procedures discussed above with respect to FIG. 4.

In column 8, Howard goes on to explain that if the most recent authentication is acceptable, then the authentication server *copies* the appropriate cookies to the client computer system and *redirects* the user's browser back to the affiliate server (step 240). The

authentication server also copies certain elements of the user's profile information to the affiliate server (step 242). The affiliate server then generates a personalized web page and communicates the web page to the user's browser (step 244). The affiliate server also copies a cookie to the client computer system containing information indicating that the user of the client computer system has been authenticated and indicating the period of time during which the authentication is valid. Each time the user enters a new web page request on the same affiliate server, the data in the cookie is copied to the affiliate server along with the page request. Thus, the affiliate server will not repeatedly check the authentication of a user during each subsequent page request.

However, these teachings are also different than the claimed invention. That is, the authentication server of Howard has no protected resource that the client may access, i.e., the authentication server is provided by Howard to control authentication, and not to provide (and allow access to) protected resources. Such goes to the nature of Howard's authentication server vis-à-vis the claimed second system.

Further, claim 1 recites retrieving, at the first system, information from a session token held by the client, the information being retrieved from the client, the information corresponding to a session credential for the second system ... and the first system presenting at least some of the information from the session token to the second system. Such features are different than Howard, in that the affiliate sever of Howard does not present such information to the authentication server.

In the Office Action, the Action asserts that Howard does not teach a session token, but alleges that it would have been obvious to use a session taken in view of wood. Applicant

submits that even if it were obvious to combine, which it is not admitted, such modification of Howard would fail to address the deficiencies as described above.

Accordingly, Applicant respectfully submits that the applied art fails to teach or suggest the invention as recited in claim 1 for at least the reasons set forth above. Further, Applicant respectfully submits that claims 9-12, 13, 17 and 20 recite patentable subject matter for reasons similar to those set forth above with respect to claim 1.

Further, the various dependent claims recite patentable subject matter at least for their various dependencies on the independent claims, as well as for the additional subject matter such dependent claims recite.

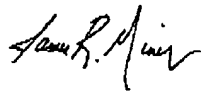
D. Conclusion

For at least the reasons outlined above, Applicant respectfully asserts that the application is in condition for allowance. Favorable reconsideration and allowance of the claims are respectfully solicited.

For any fees due in connection with filing this Response the Commissioner is hereby authorized to charge the undersigned's Deposit Account No. 50-0206.

Should the Examiner believe anything further is desirable in order to place the application in even better condition for allowance, the Examiner is invited to contact Applicant's undersigned representative at the telephone number listed below.

Respectfully submitted,
HUNTON & WILLIAMS



James R. Miner
Registration No. 40,444

Hunton & Williams
1900 K Street, N.W., Suite 1200
Washington, D.C. 20006-1109
(202) 955-1500

Dated: **August 24, 2006**